

AMENDMENTS TO THE CLAIMS

This Listing of Claims will replace all prior versions and listings of claims in this application.

Listing of Claims:

1. (Previously Presented) An apparatus, comprising:
a plurality of ports to at least one of which a terminal or network having an encrypting capability can be directly or indirectly connected;
encryption/decryption means for performing an encrypting process to apply encryption-based security and a decrypting process to remove encryption-based security on data being communicated between the terminal or network having the encrypting capability and another network or terminal coupled to one of the plurality of ports; and
bridge means in a data link layer for allowing data, which has been received with one of the plurality of ports and then on which the encrypting or decrypting process has been performed, to be outputted as it is from another port without any routing process at a network layer being performed, the bridge means being disposed within the apparatus, along with the encryption/decryption means.
2. (Previously Presented) The apparatus according to claim 1, wherein the encryption/decryption means is adapted to perform the encrypting process and the decrypting process on data, so that the apparatus receives and retransmits data in the form of encrypted data from and to the terminal or network having the encrypting capability, and the apparatus receives and retransmits the data in the form of non-encrypted data from and to a network or apparatus coupled to another port of the apparatus and having no encrypting capability.
3. (Previously Presented) An apparatus, comprising:
a plurality of ports to at least one of which a terminal or network can be directly or indirectly connected;

encryption/decryption means for performing an encrypting process or a decrypting process on data which has been received with one of the plurality of ports and then has passed through a physical layer and a data link layer, the encrypting process or decrypting process generating encrypted data or decrypted data; and

bridge means in the data link layer for passing the encrypted data or decrypted data to the data link layer and the physical layer without passing said data to a network layer in which routing between networks is controlled, and then sending said data to another port so as to be outputted from said port to another terminal or network coupled to the other port, the bridge means being disposed within the apparatus, along with the encryption/decryption means.

4. (Previously Presented) The apparatus according to claim 3, further comprising setting information storage means for storing setting information for controlling the encrypting process and the decrypting process, wherein the encryption/decryption means controls the encrypting process and the decrypting process by comparing the setting information stored in the setting information storage means with header information of a data packet of data received with one of the plurality of ports.

5. (Previously Presented) A method for performing an encrypting process and a decrypting process using an encryption/decryption apparatus, comprising:

performing the encrypting or decrypting process on data which has been received with a first one of a plurality of ports of the encryption/decryption apparatus from a first network or terminal coupled to the first one of the plurality of ports and then has passed through a data link layer and a physical layer of the encryption/decryption apparatus, to thereby obtain encrypted data or decrypted data; and

outputting the encrypted data or decrypted data from a second one of the plurality of ports of the encryption/decryption apparatus through the physical layer and bridge means in the data link layer of the encryption/decryption apparatus to a second network or terminal coupled to the second one of the plurality of ports, without passing said data to a network layer in which routing is controlled.

6. (Previously Presented) A system, comprising:
the apparatus according to claim 1; and
a terminal or network having an encrypting capability which can be connected to the apparatus.
7. (Previously Presented) A system, comprising:
a terminal or network having an encrypting capability;
a terminal or network having no encrypting capability; and
the apparatus according to claim 2 which can be connected between the terminal or network having the encrypting capability and the terminal or network having no encrypting capability.
8. (Previously Presented) The apparatus according to claim 2, wherein the encryption/decryption means is configured to perform the decrypting process on encrypted data and then sends said data to a terminal or network having no encrypting capability when the apparatus receives said encrypted data from another terminal or network having an encrypting capability and retransmits said data to the terminal or network having no encrypting capability, and is configured to perform the encrypting process on non-encrypted data and then send said data to a terminal or network having an encrypting capability when the apparatus receives said non-encrypted data from another terminal or network having no encrypting capability and retransmits said data to the terminal or network having the encrypting capability.
9. (Previously Presented) The apparatus of claim 1, wherein the bridge means is an IP-Sec bridge and data transmission processes are carried out in layers lower than the network layer.
10. (Previously Presented) The apparatus of claim 3, wherein the bridge means is an IP-Sec bridge and data transmission processes are carried out in layers lower than the network layer.

11. (Previously Presented) The method of claim 5, wherein the bridge means is an IP-Sec bridge and data transmission processes are carried out in layers lower than the network layer.

12. (Previously Presented) The method according to claim 5, wherein said performing the encrypting or decrypting process comprises:

performing the encrypting process and the decrypting process on data so that data is received from or transmitted to a terminal or network having encryption capability in the form of encrypted data and so that data is received from or transmitted to a terminal or network without encryption capability in the form of non-encrypted data.

13. (Previously Presented) The method according to claim 12, wherein said performing the encrypting process and the decrypting process comprises:

performing the decrypting process on encrypted data received from a terminal or network having encryption capability and destined for a terminal or network not having encryption capability;

performing the encrypting process on data received from a terminal or network not having encryption capability and destined for a terminal or network having encryption capability.

14. (Previously Presented) The method according to claim 5, further comprising controlling the encrypting process and the decrypting process by comparing setting information stored in the encryption/decryption apparatus with header information of a data packet of data received with one of the plurality of ports.

15. (Previously Presented) The method according to claim 5, wherein said outputting comprises outputting the encrypted data if the second terminal or network has encryption capability and outputting the decrypted data if the second terminal or network does not have encryption capability.

16. (Previously Presented) The apparatus according to claim 3, wherein the other network or terminal coupled to the other port has encryption capability in the case in which the encrypted

data is passed and does not have encryption capability in the case in which the decrypted data is passed.

17. (New) The apparatus according to claim 1, wherein the apparatus is configured to process data received with one of the plurality of ports without changing a network address of a destination associated with the data.

18. (New) The apparatus according to claim 3, wherein the apparatus is configured to process data received with one of the plurality of ports without changing a network address of a destination associated with the data.

19. (New) The method according to claim 5, wherein the data received with the first one of the plurality of ports is output, following the performing of the encrypting or decrypting process, without changing a network address of a destination associated with the data.